Aulão

NAT e **CGNAT**

Redes Brasil

Instrutor

Nome: Francisco Neto

Resumo:

- Trabalha com telecomunicações desde 2005.
- Trabalhou na OI como administrador de redes.
- Sócio de um provedor de internet em Goiás;
- Possui certificações da MikroTik, Ubiquiti, Huawei e outros;
- Instrutor oficial MikroTik (Certificado de Trainer TR0184).

Cronograma Aulão NAT e CGNAT

Redes Brasil

- Porque usar NAT e porque CGNAT?
- Os canais do NAT do MikroTik RouterOS.
- Entendendo como funciona o SRC-NAT + boas práticas.
- Entendendo como funciona o DST-NAT + boas práticas.
- Topologias para CGNAT.
- Exemplos práticos de CGNAT com e sem uso de logs.
- Bônus final

Porque usar NAT ?

- Surgiu na década 90 como técnica paliativa para resolver o problema do escassez do IPv4;
- Foi definido na RFC 3022;
- Os prefixos abaixo foram definidas na RFC 1918 e são normalmente usados em redes que fazem uso de NAT;
  - 10.0.0.0/8
  - 192.168.0.0/16
  - 172.16.0.0/12
- O usuário final que antes recebia um bloco de IPs públicos passa a receber somente 1 IP público.

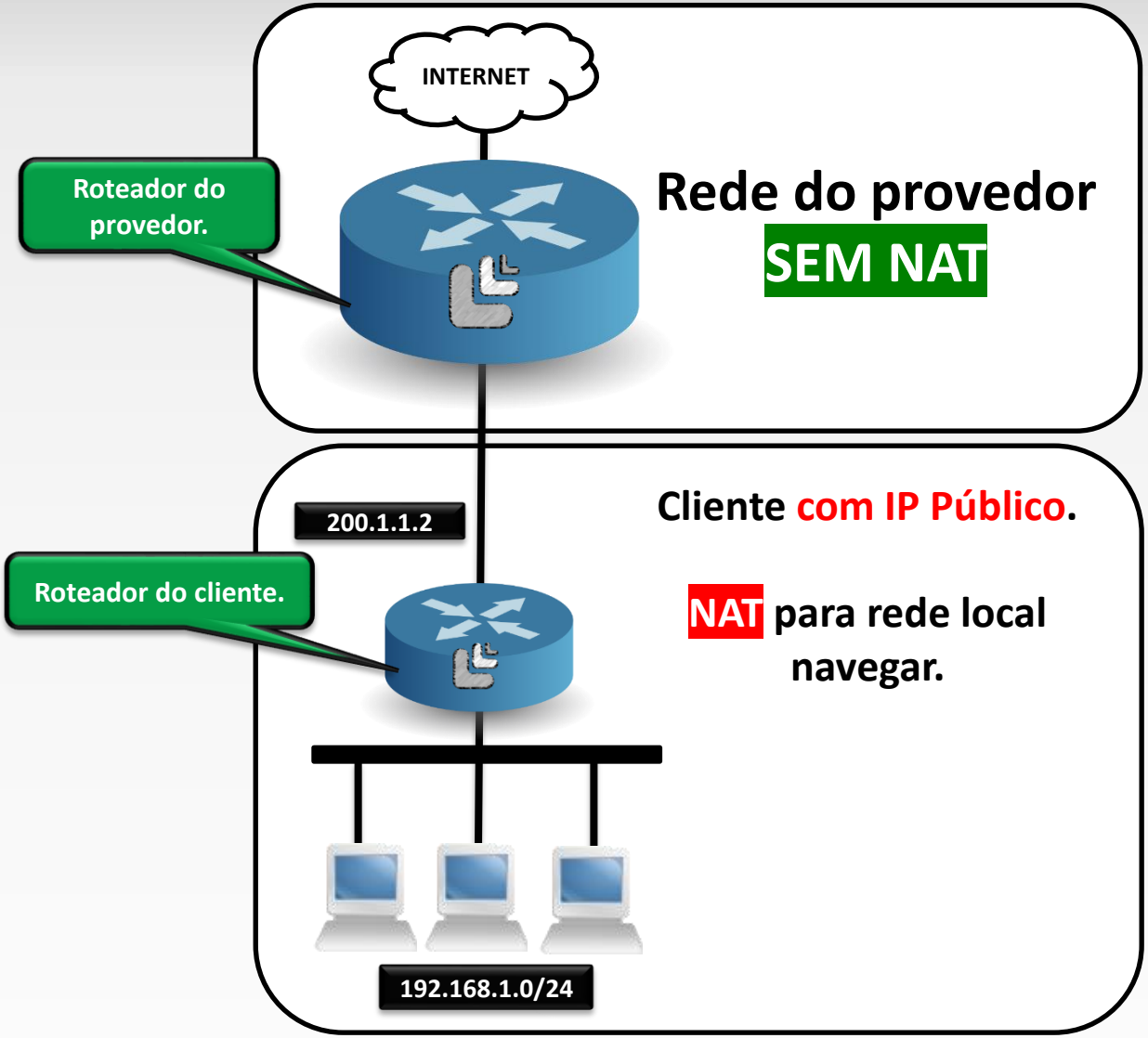
Porque usar CGNAT ?

Redes Brasil

- O CGNAT, ou Carrier Grade NAT de forma resumida é nada mais nada menos, que o uso de mais um NAT na rede do provedor;
- Definido na RFC 6598;
- A rede 100.64.0.0/10 foi definida na para atender as necessidade de CGNAT;
- O usuário final que antes recebia 1 IP público já na recebe mais.

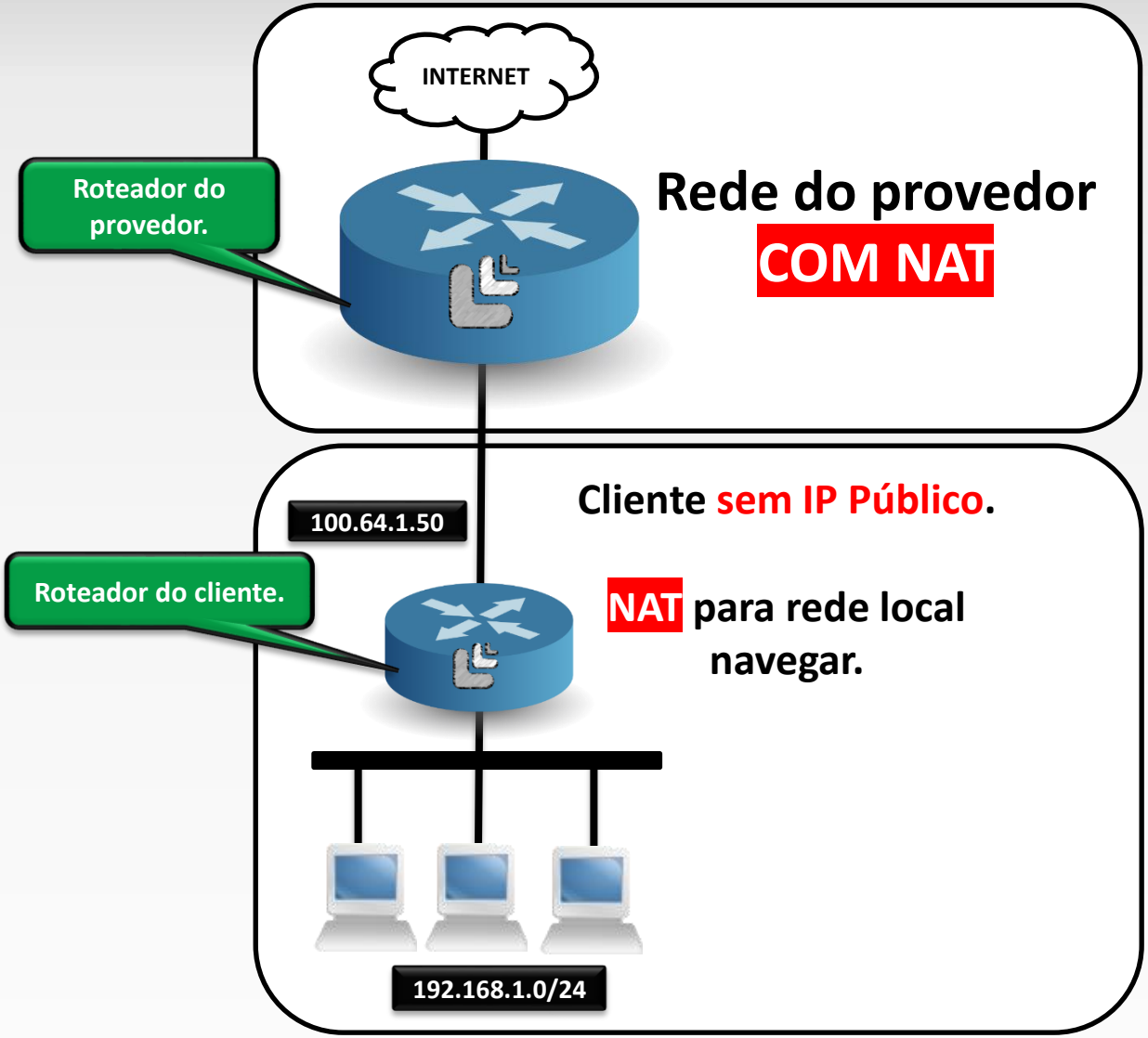
Rede sem CGNAT

Redes Brasil



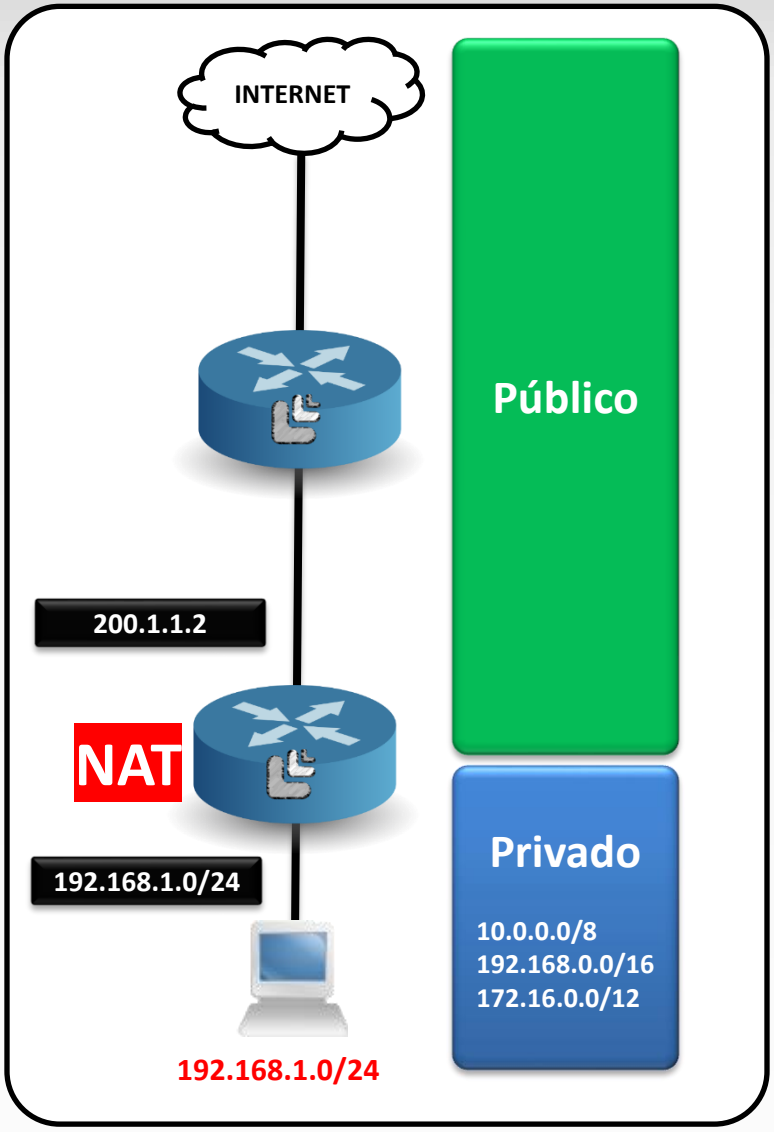
Rede com CGNAT

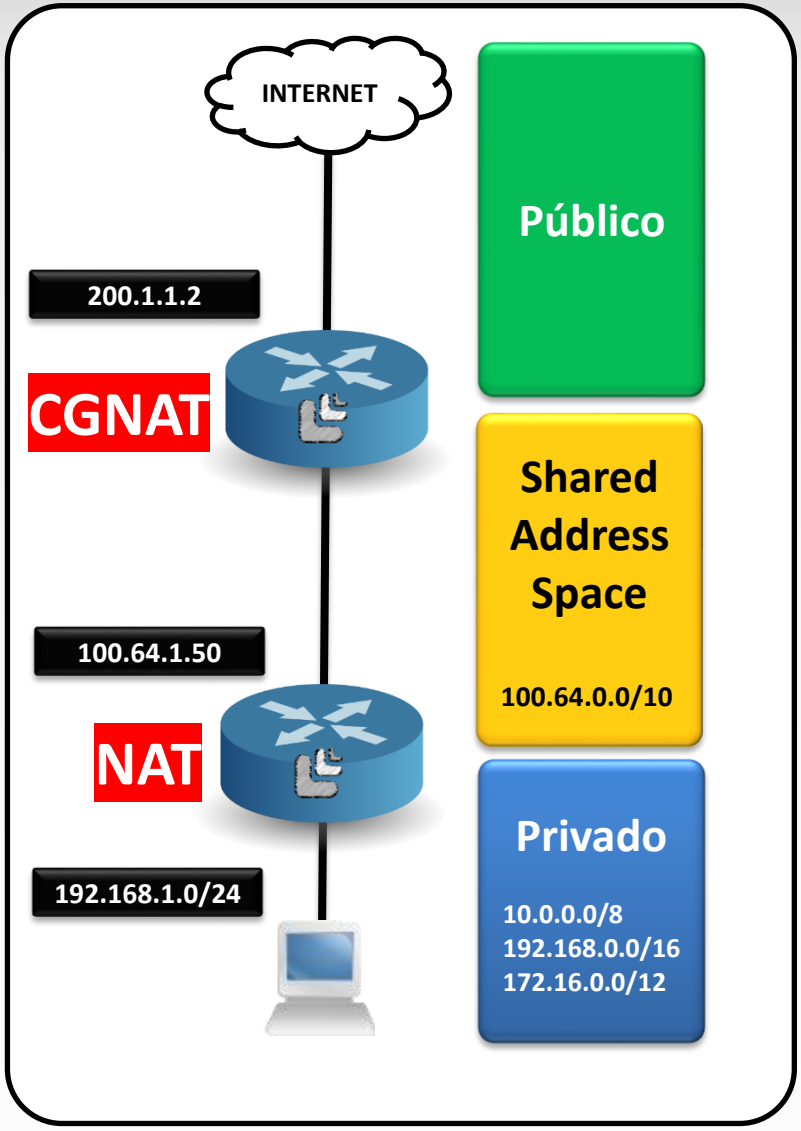
Redes Brasil



NAT vs CGNAT

Redes Brasil



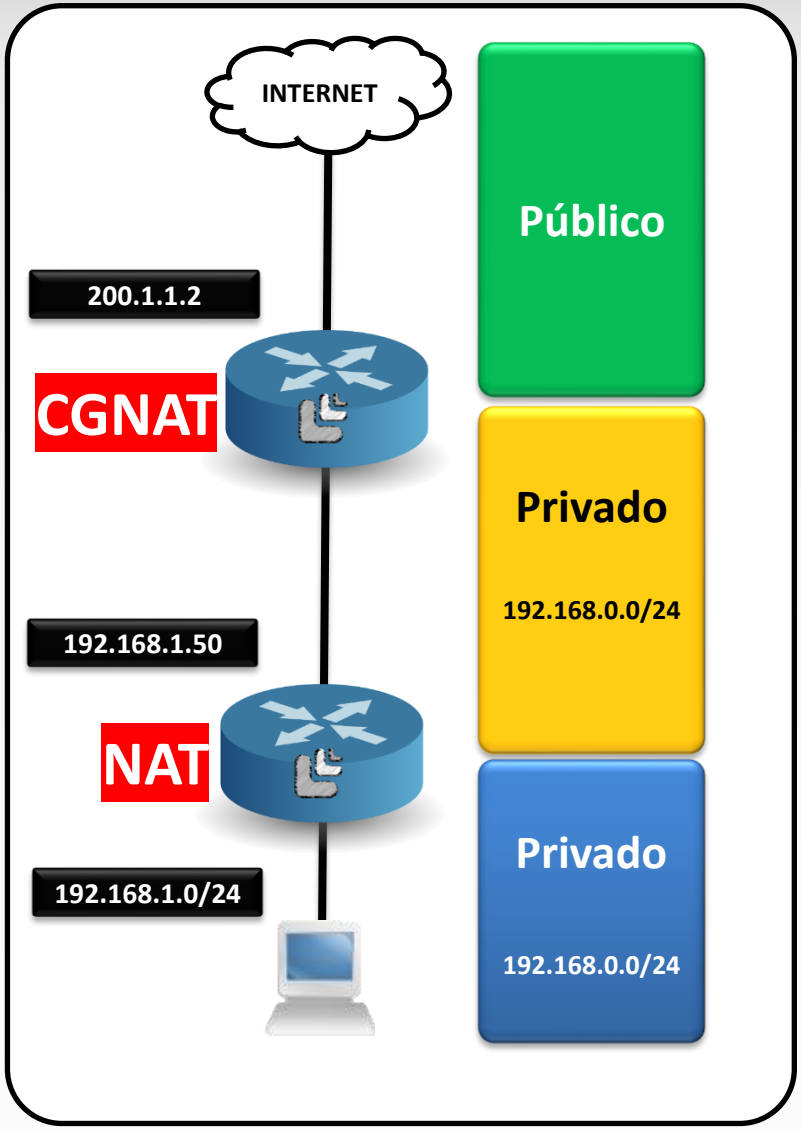


NAT vs CGNAT

Redes Brasil

- Porque usar a rede 100.64.0.0/10 ?

- Posso usar a faixa de rede privada ?

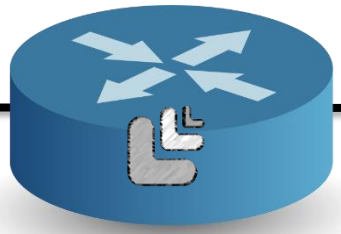


Cronograma Aulão NAT e CGNAT

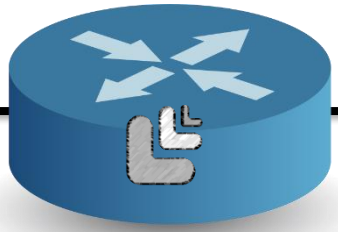
- Porque usar NAT e porque CGNAT?
- Os canais do NAT do MikroTik RouterOS.
- Entendendo como funciona o SRC-NAT + boas práticas.
- Entendendo como funciona o DST-NAT + boas práticas.
- Topologias para CGNAT.
- Exemplos práticos de CGNAT com e sem uso de logs.
- Bônus final

Cases mais comuns de uso do NAT

Redes Brasil



Host com **IP privado** se comunicando com host que possui **IP público**.



Host com **IP público** se comunicando com host que possui **IP privado**.

Entendo os canais do NAT

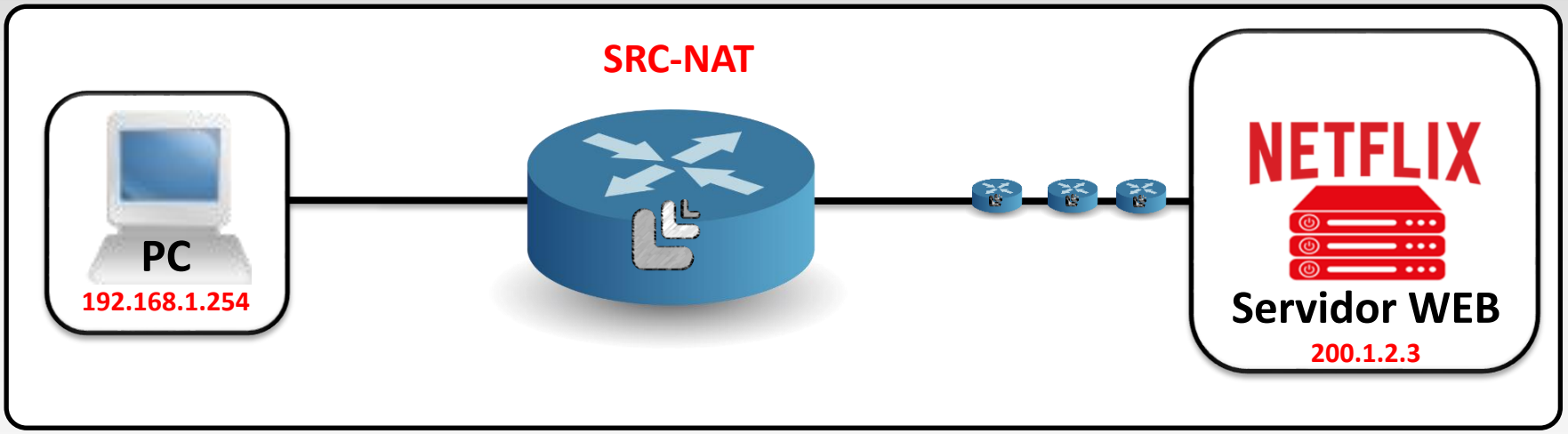
Redes Brasil

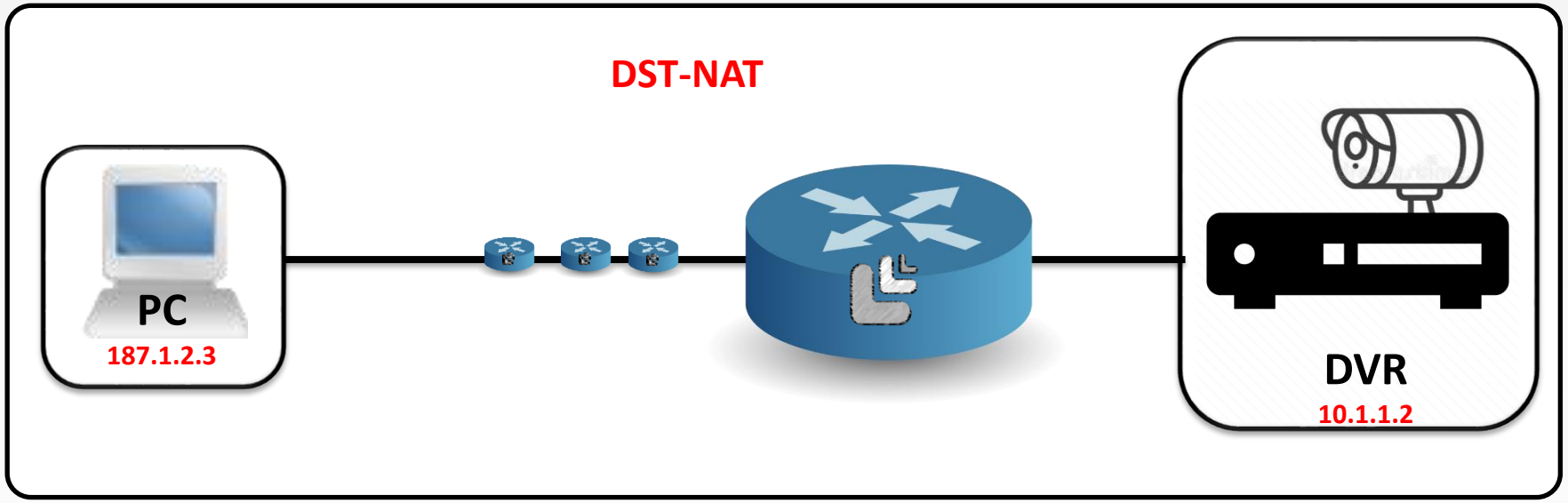
SRC-NAT: O roteador faz tradução do IP e/ou porta de origem.

DST-NAT: O roteador faz tradução do IP e/ou porta de destino.

Cases mais comuns de uso do NAT

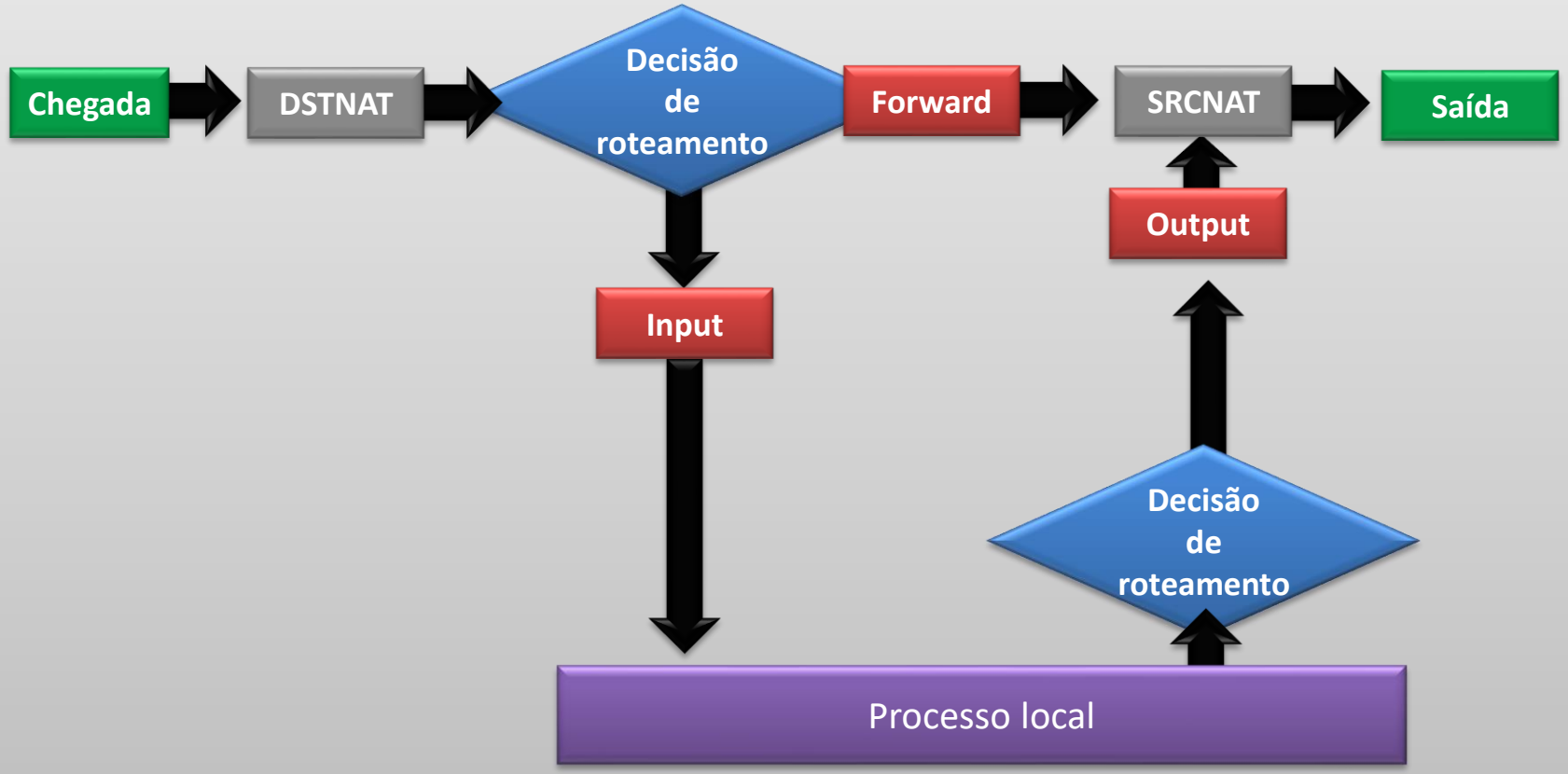
Redes Brasil





Localização DST-NAT e SRC-NAT

Firewall

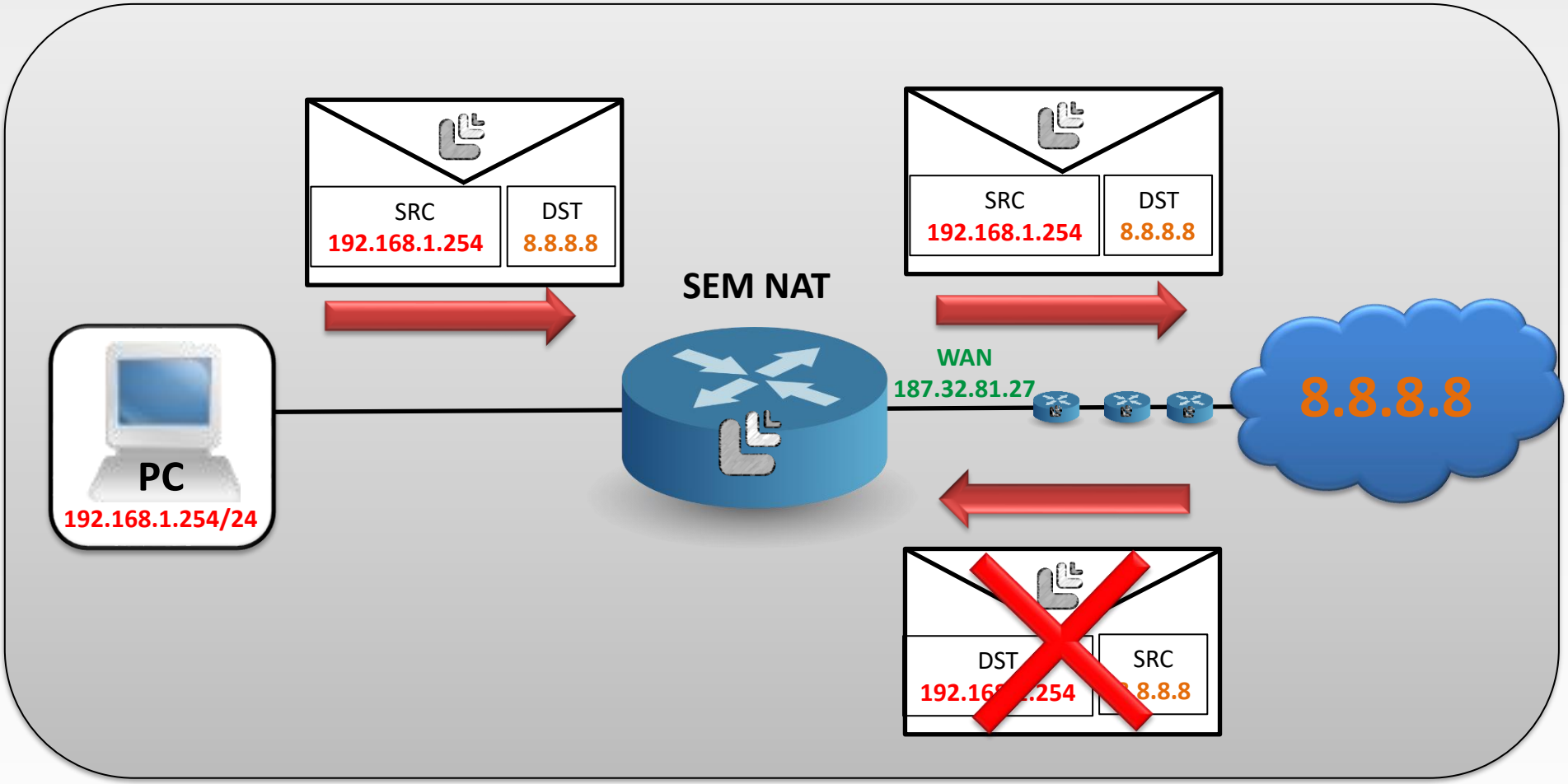


Cronograma Aulão NAT e CGNAT

Redes Brasil

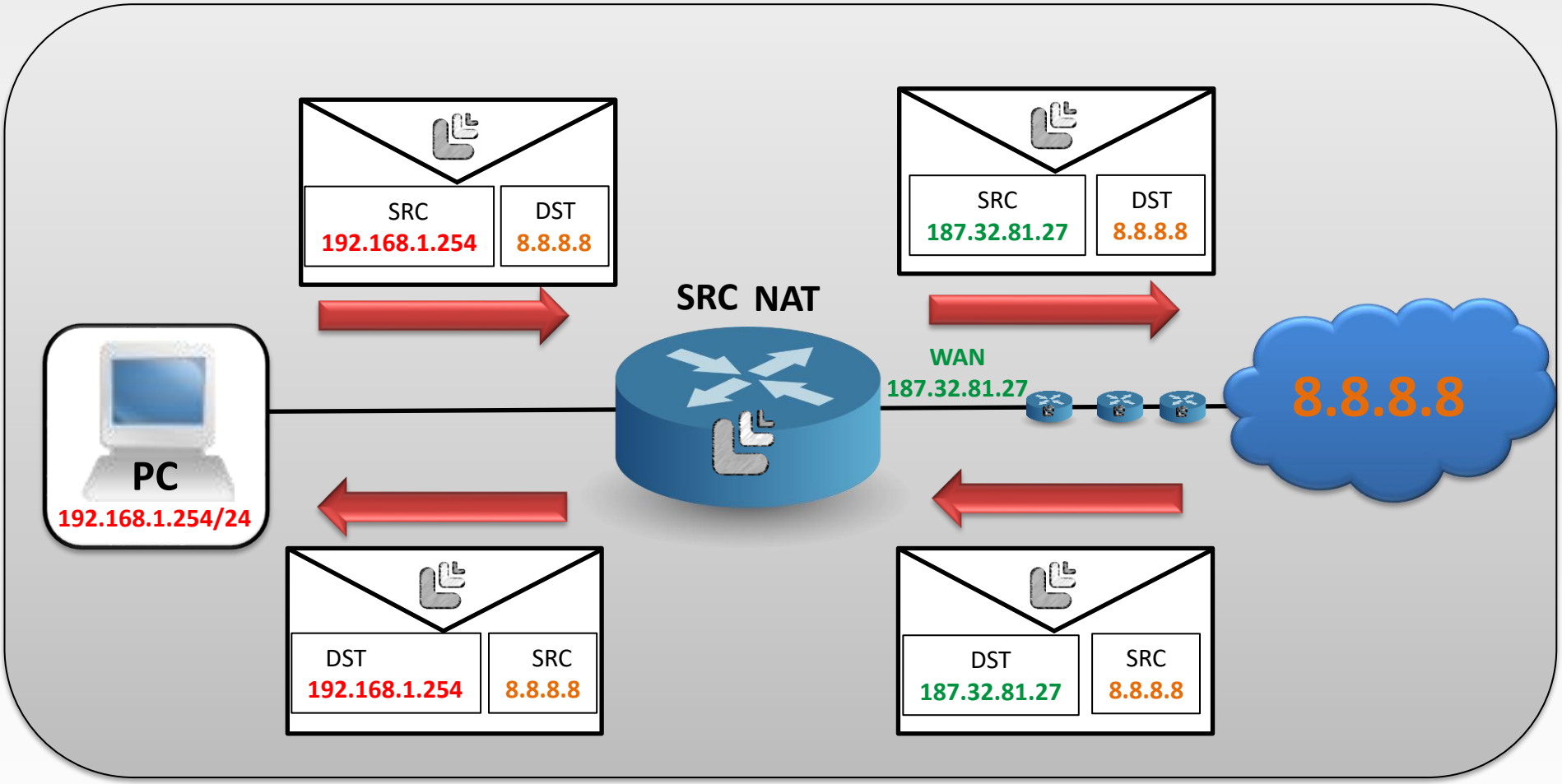
- ✓ Porque usar NAT e porque CGNAT?
- ✓ Os canais do NAT do MikroTik RouterOS.
- Entendendo como funciona o SRC-NAT + boas práticas.
- Entendendo como funciona o DST-NAT + boas práticas.
- Topologias para CGNAT.
- Exemplos práticos de CGNAT com e sem uso de logs.
- Bônus final

SRC-NAT

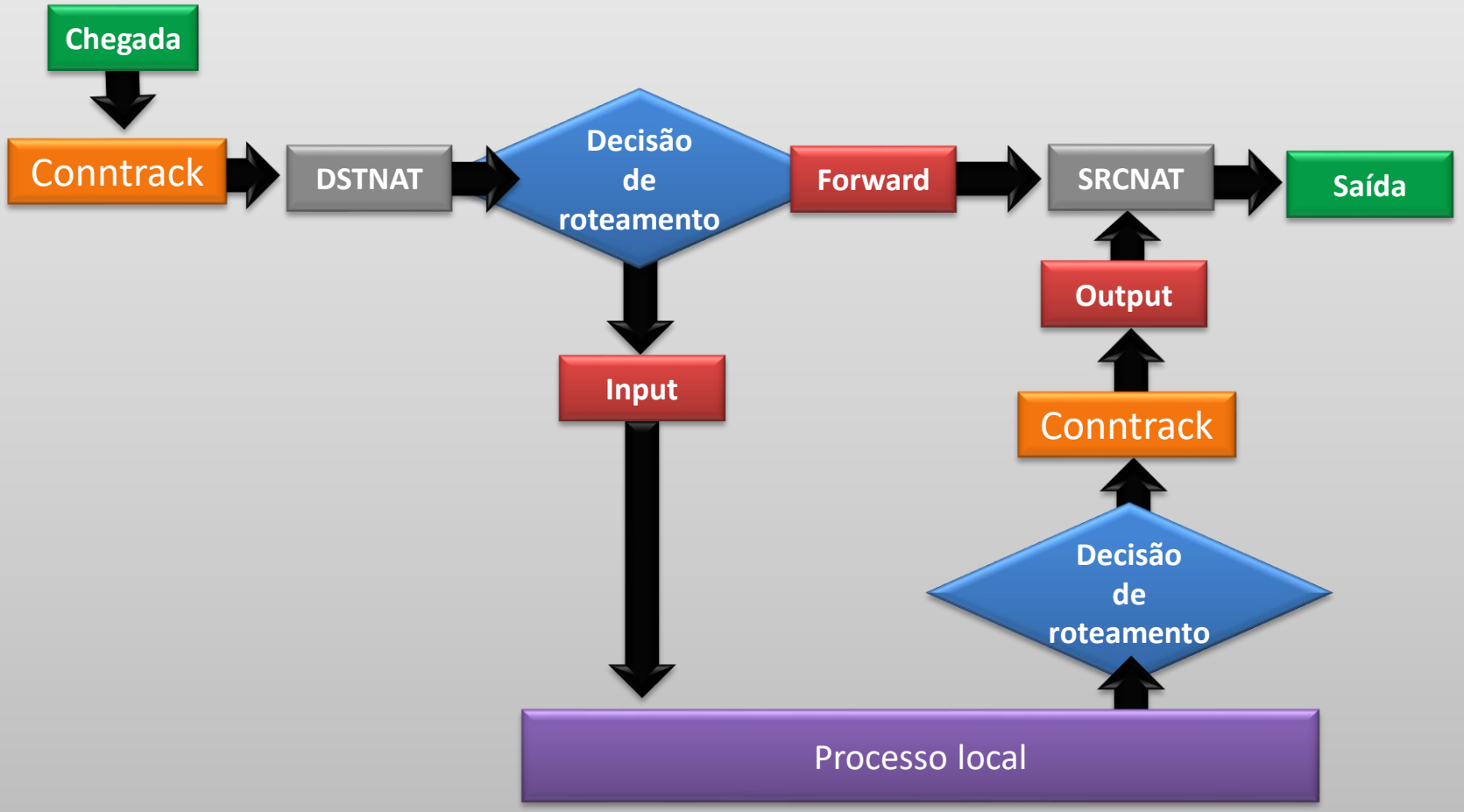

SRC
192.168.1.254
DST
8.8.8.8
SEM NAT
SRC
192.168.1.254
DST
8.8.8.8
WAN
187.32.81.27
8.8.8.8
PC
192.168.1.254/24
DST
SRC
8.8.8.8

SRC-NAT

Redes Brasil



Localização da Connection Tracking



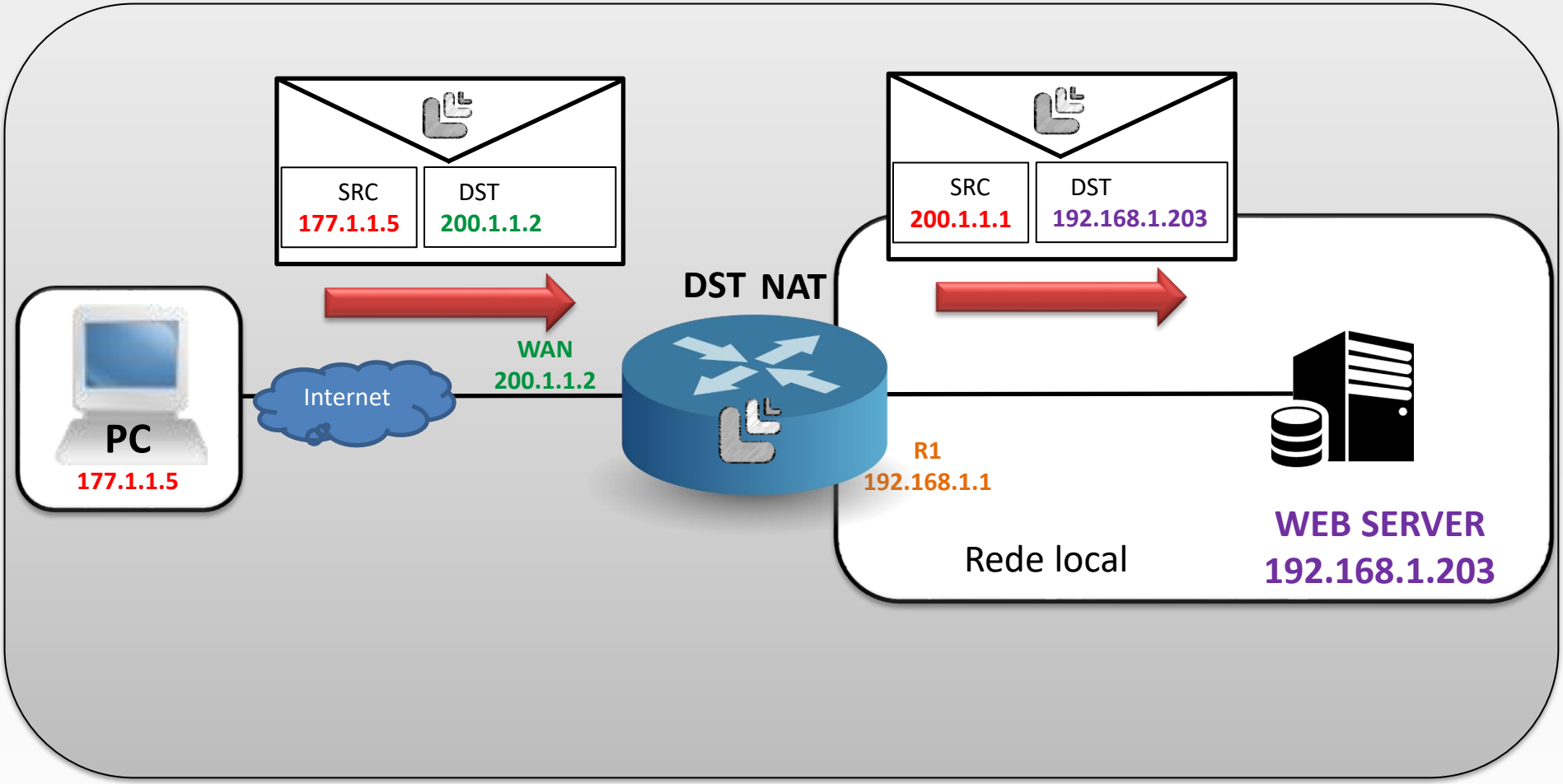
Cronograma Aulão NAT e CGNAT

Redes Brasil

- [x] Porque usar NAT e porque CGNAT?
- [x] Os canais do NAT do MikroTik RouterOS.
- [x] Entendendo como funciona o SRC-NAT + boas práticas.
- [ ] Entendendo como funciona o DST-NAT + boas práticas.
- [ ] Topologias para CGNAT.
- [ ] Exemplos práticos de CGNAT com e sem uso de logs.
- [ ] Bônus final

DSTNAT

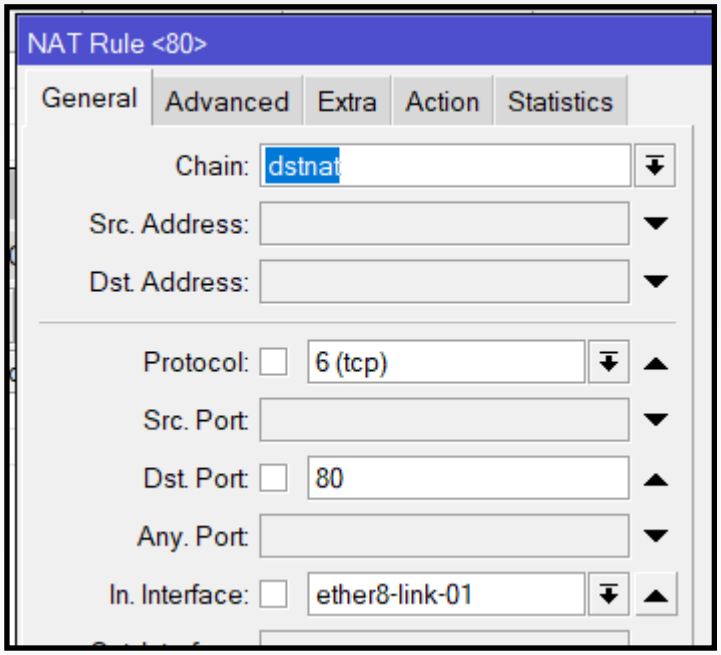
Redes Brasil

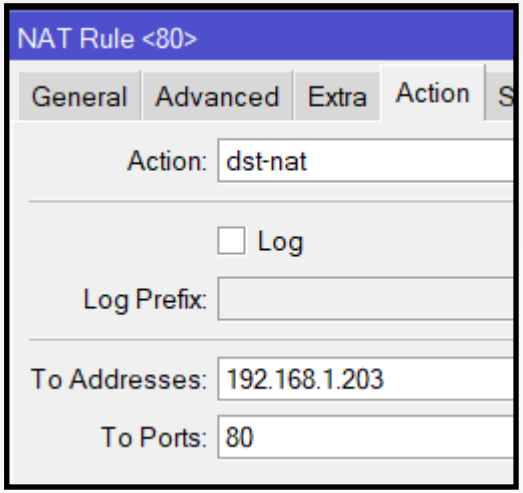


Ação DST-NAT e redirecionamento

Redes Brasil

- Redirecionamento de portas para acessar externamente um servidor WEB que não possui IP público.





Cronograma Aulão NAT e CGNAT

Redes Brasil

- ✓ Porque usar NAT e porque CGNAT?
- ✓ Os canais do NAT do MikroTik RouterOS.
- ✓ Entendendo como funciona o SRC-NAT + boas práticas.
- ✓ Entendendo como funciona o DST-NAT + boas práticas.
- Topologias para CGNAT.
- Exemplos práticos de CGNAT com e sem uso de logs.
- Bônus final

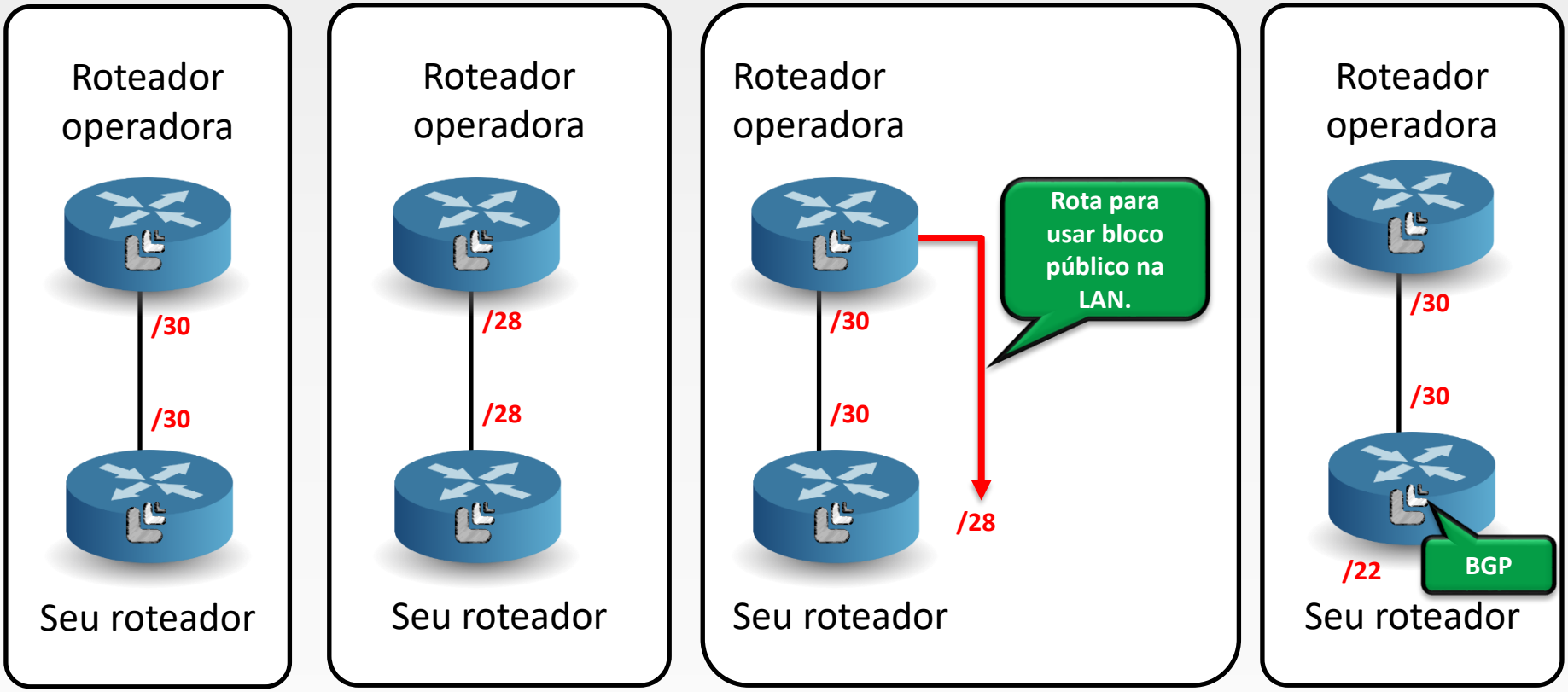
CGNAT

- Cada rede tem suas particularidades;

- O ideal é você conhecer as diversas topologias e possibilidades de forma que não fique preso a somente um desenho de rede.

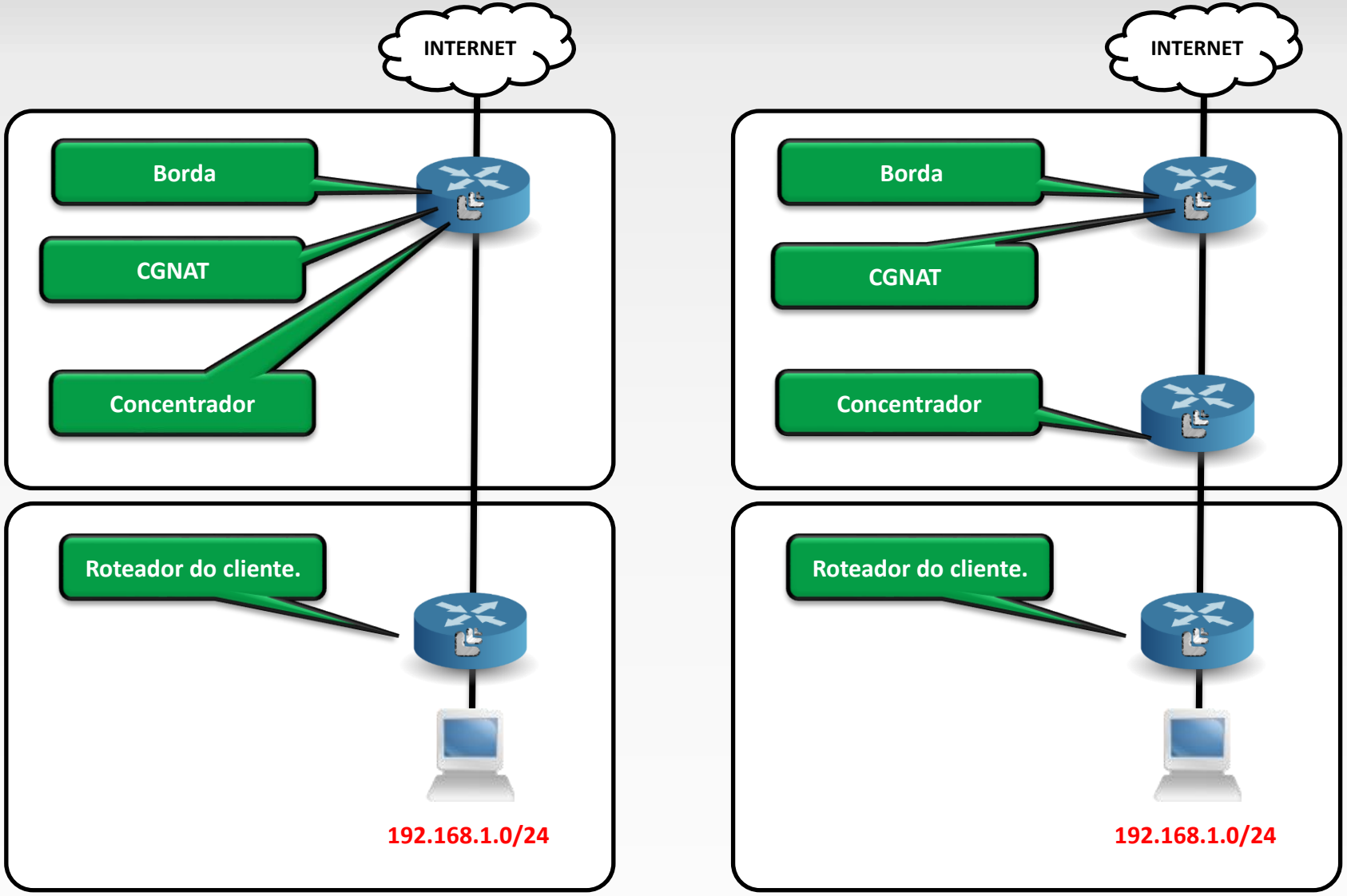
Quantos IPs públicos você tem ?

Redes Brasil



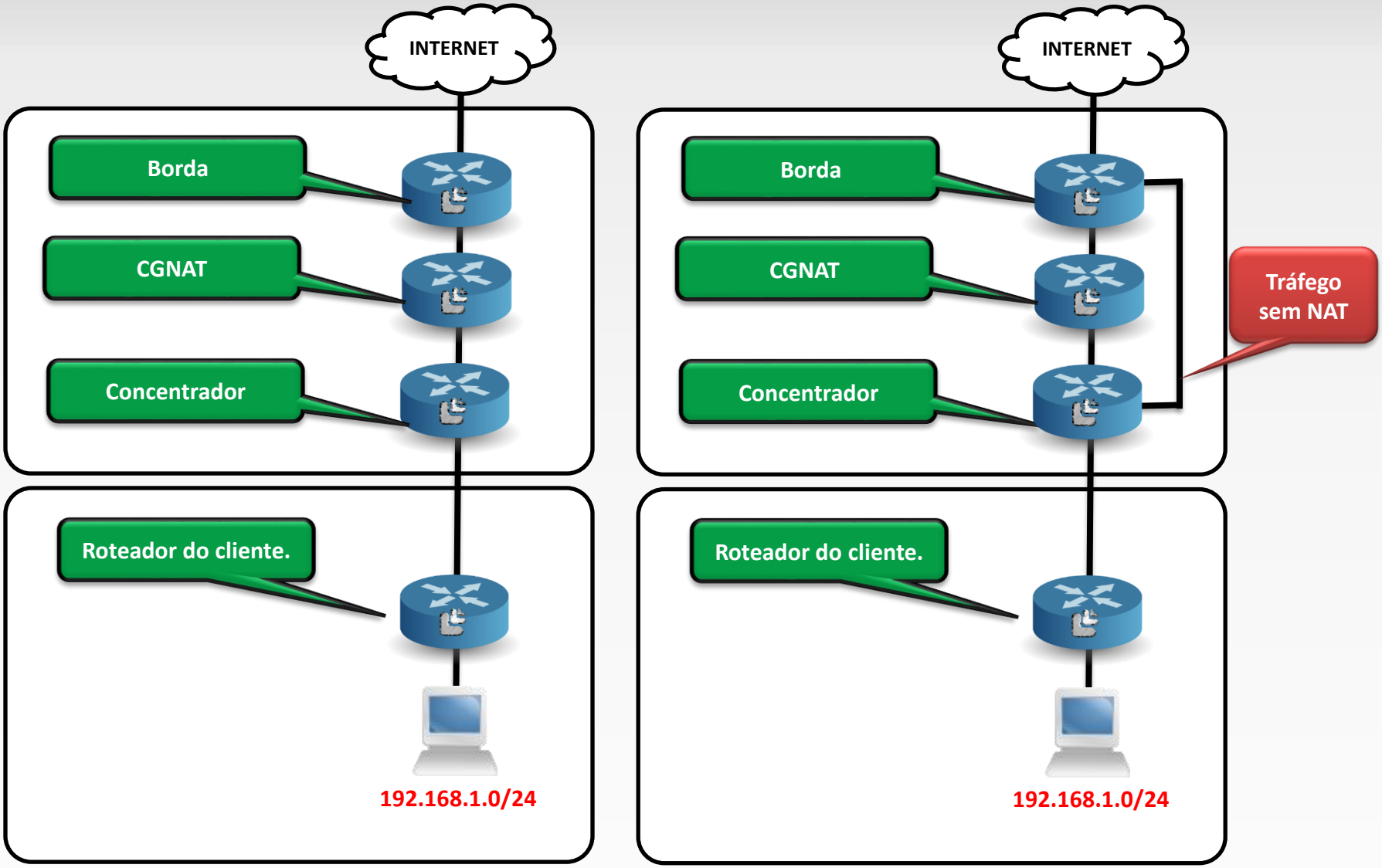
Topologias

Redes Brasil

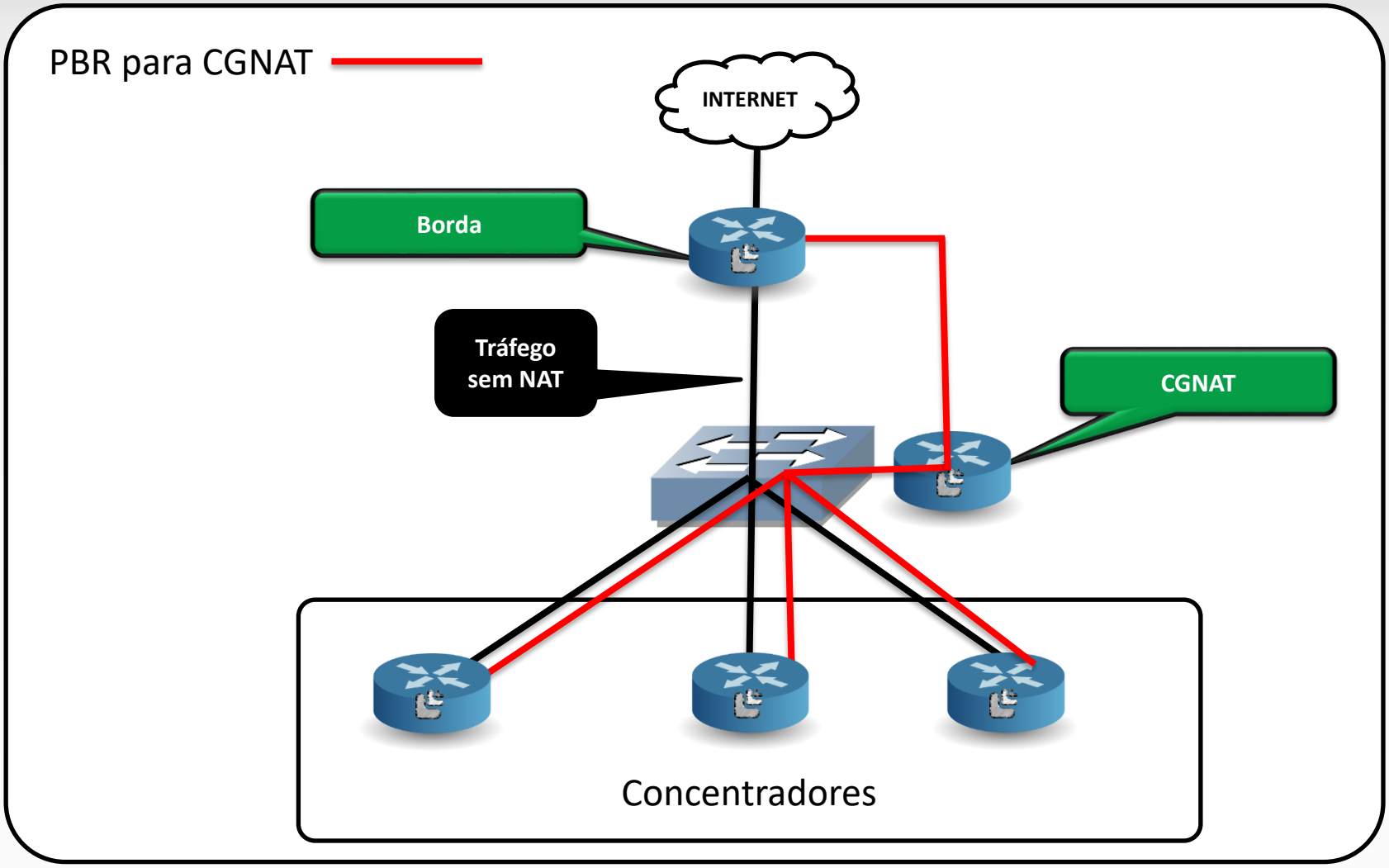


Topologias

Redes Brasil

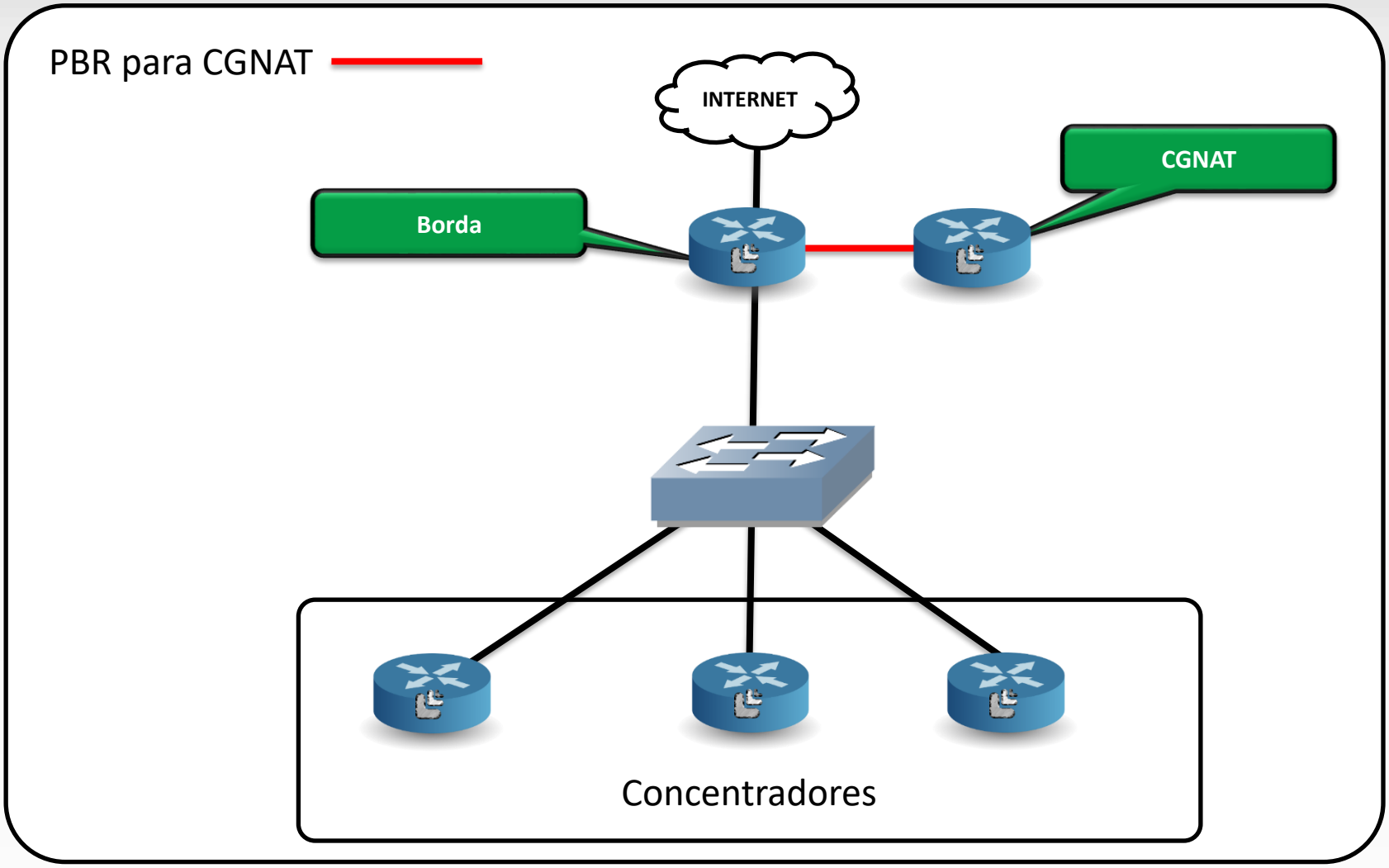


Topologias

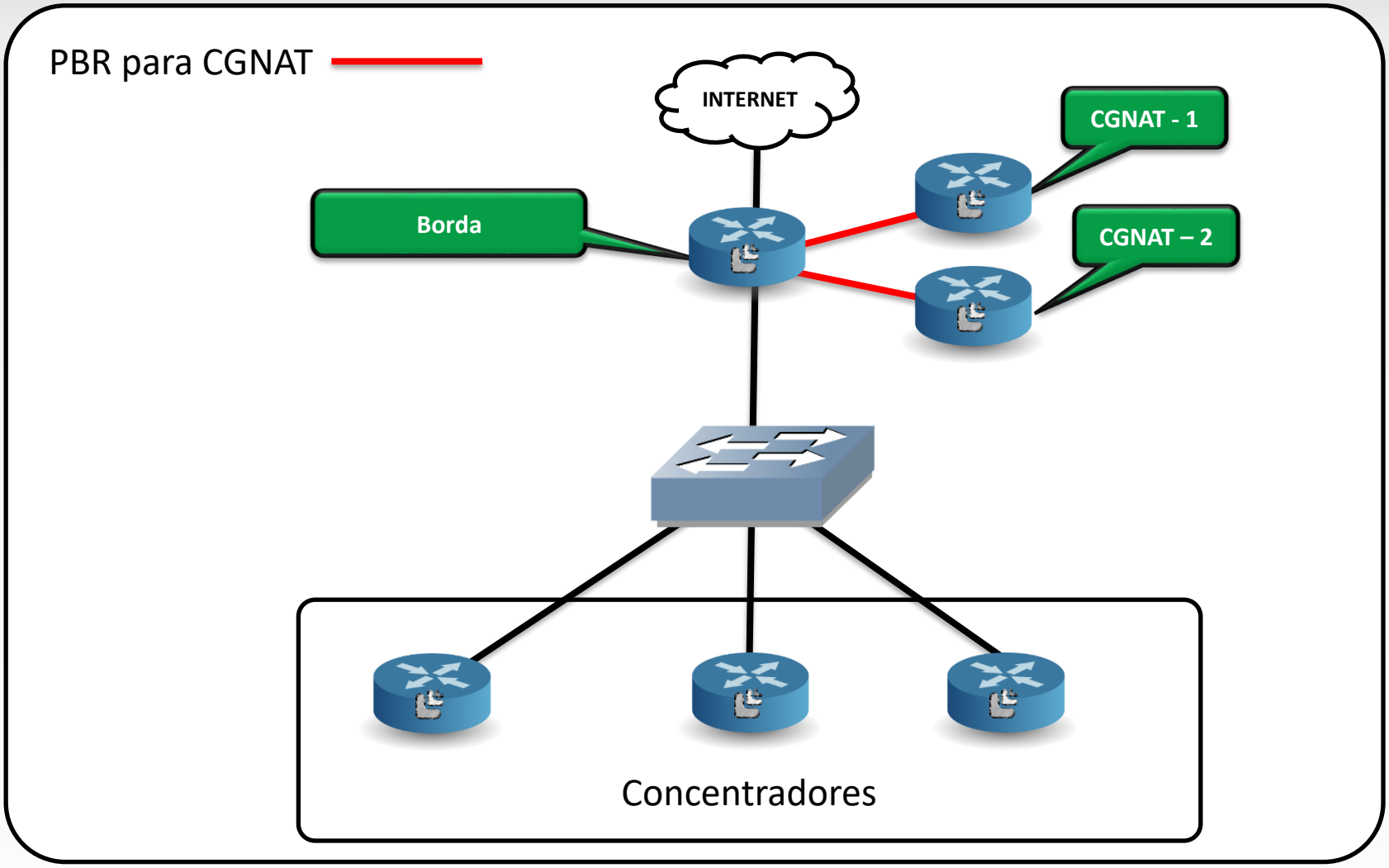

PBR para CGNAT
INTERNET
Borda
Tráfego
sem NAT
CGNAT
Concentradores

Topologias

Redes Brasil



Topologias


PBR para CGNAT
INTERNET
CGNAT - 1
Borda
CGNAT – 2
Concentradores

Cronograma Aulão NAT e CGNAT

- [x] Porque usar NAT e porque CGNAT?
- [x] Os canais do NAT do MikroTik RouterOS.
- [x] Entendendo como funciona o SRC-NAT + boas práticas.
- [x] Entendendo como funciona o DST-NAT + boas práticas.
- [x] Topologias para CGNAT.
- [ ] Exemplos práticos de CGNAT com e sem uso de logs.
- [ ] Bônus final

CGNAT

- Existem várias maneiras de se implementar CGNAT no RouterOS;

- O ideal é que você conheça cada possibilidade para fazer a melhor escolha de acordo com a sua necessidade.

COM ou SEM Logs

Redes Brasil

Alocação dinâmica de portas

- Será necessário guardar logs com a porta de origem de cada conexão;
- Será necessário guardar logs de autenticação e atribuição de IPs;
- Maior economia de IPs públicos.

Alocação estática de portas

- Não será necessário guardar logs com a porta de origem de cada conexão;
- Será necessário guardar logs de autenticação e atribuição de IPs.
- Menor economia de IPs públicos.

Ações usadas no canal SRC-NAT

- **Masquerade:** Altera o endereço de IP de origem usando o IP da interface de saída.
- **SRC-NAT:** Altera o endereço de IP e/ou porta de origem por um IP e/ou porta de sua escolha. O campo to-address aceita range e rede, e a distribuição das traduções acontece de forma completamente aleatória.
- **SAME**: Altera o endereço de IP e/ou porta de origem por um IP e/ou porta de sua escolha. O campo to-address aceita range e rede, e a distribuição das traduções mantém o IP selecionado para conexões com mesmo IP de origem e mesmo IP de destino.
- **NETMAP:** Faz mapeamento de endereços, ação geralmente utilizada para mapear IPs privados em IPs públicos. O campo to-address aceita somente endereço de rede, e a distribuição das traduções acontece literalmente de forma mapeada.

CGNAT com ação SRC-NAT

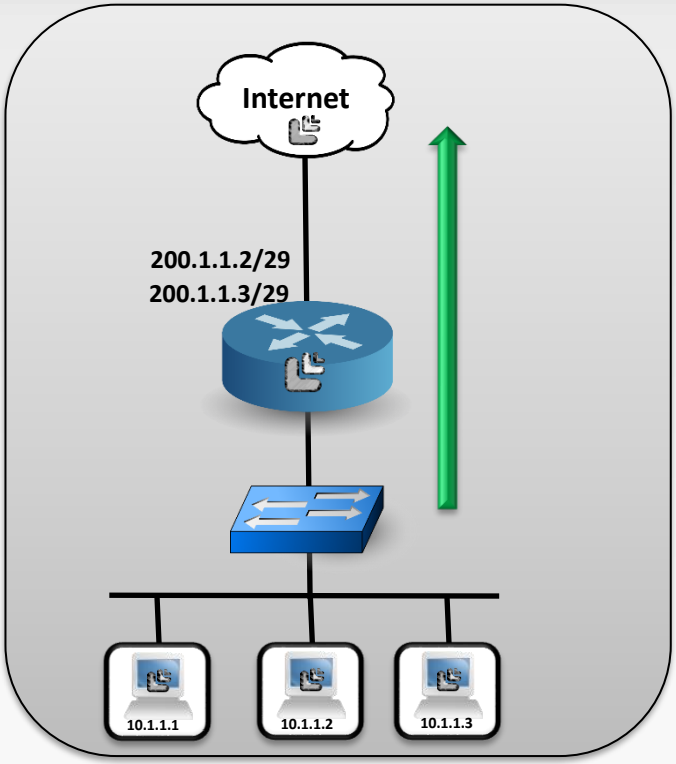
- Indicado quando irá usar somente um IP público em cada regra, para as traduções dos IPs privados;

- Recomendado para cenários mais simples,

Usando a ação SRC-NAT

Redes Brasil

- **Forçando mascaramento ser feito por um endereço de IP de sua escolha.**



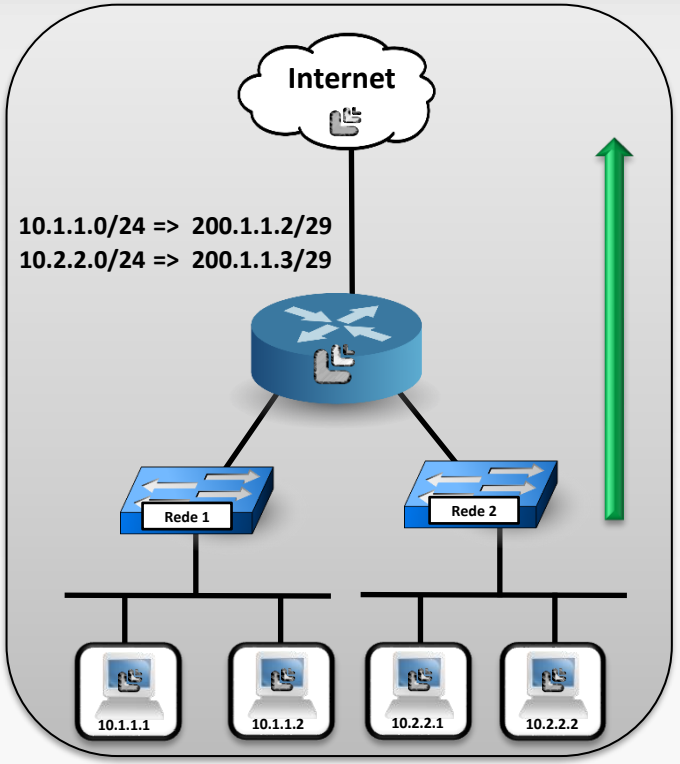
Comandos

```
/ip firewall nat
add action=src-nat chain=srcnat comment="For\E7ando mascaramento da rede local para o end. 200.1.1.2" dst-address-list=!rede-local dst-address-type=!multicast \
   src-address-list=rede-local to-addresses=200.1.1.2
```

Usando a ação SRC-NAT

Redes Brasil

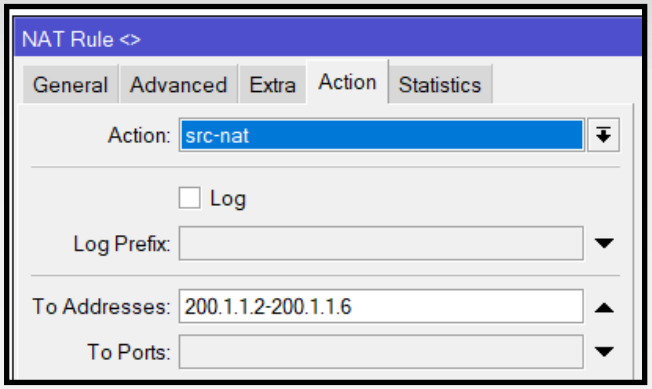
- **Forçado um IP público para cada sub-rede**

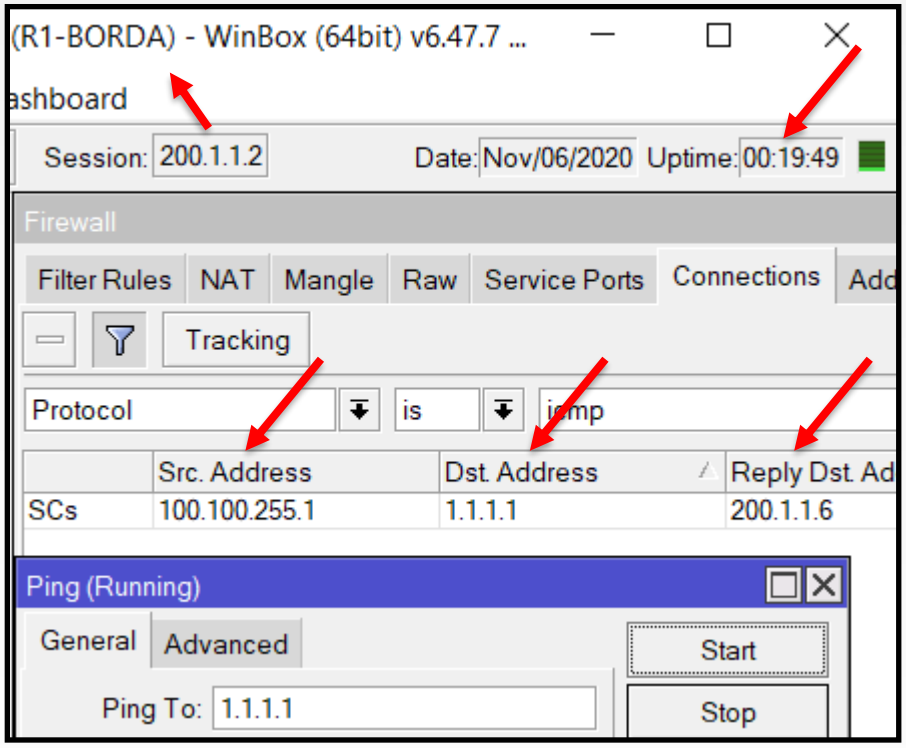


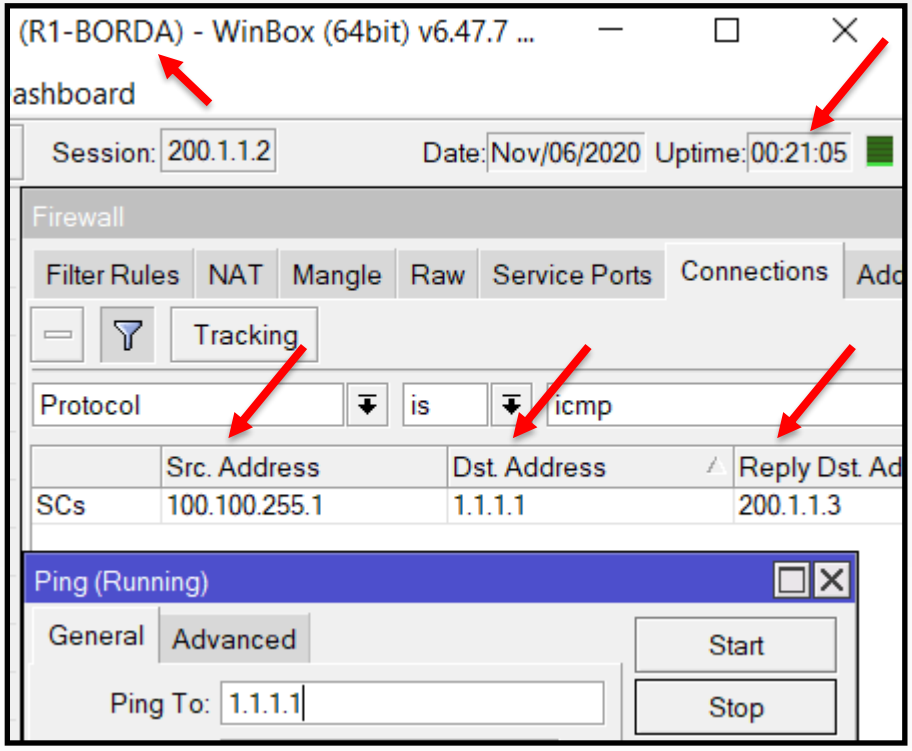
Comandos

```
/ip firewall nat
add action=src-nat chain=srcnat comment="For\E7ando mascaramento da rede local 10.1.1.0/24 para o end. 200.1.1.1" dst-address-list=!rede-local dst-address-type=\
    !multicast src-address=10.1.1.0/24 to-addresses=200.1.1.2
add action=src-nat chain=srcnat comment="For\E7ando mascaramento da rede local 10.2.2.0/24 para o end. 200.1.1.2" dst-address-list=!rede-local dst-address-type=\
    !multicast src-address=10.2.2.0/24 to-addresses=200.1.1.3
```

Problemas com SRC-NAT







CGNAT com ação SAME

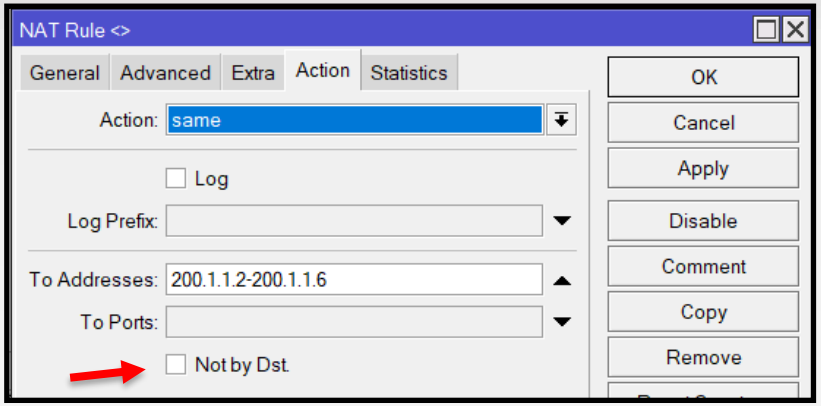
- Indicado quando irá usar vários IPs públicos na mesma regra, para as traduções dos IPs privados.

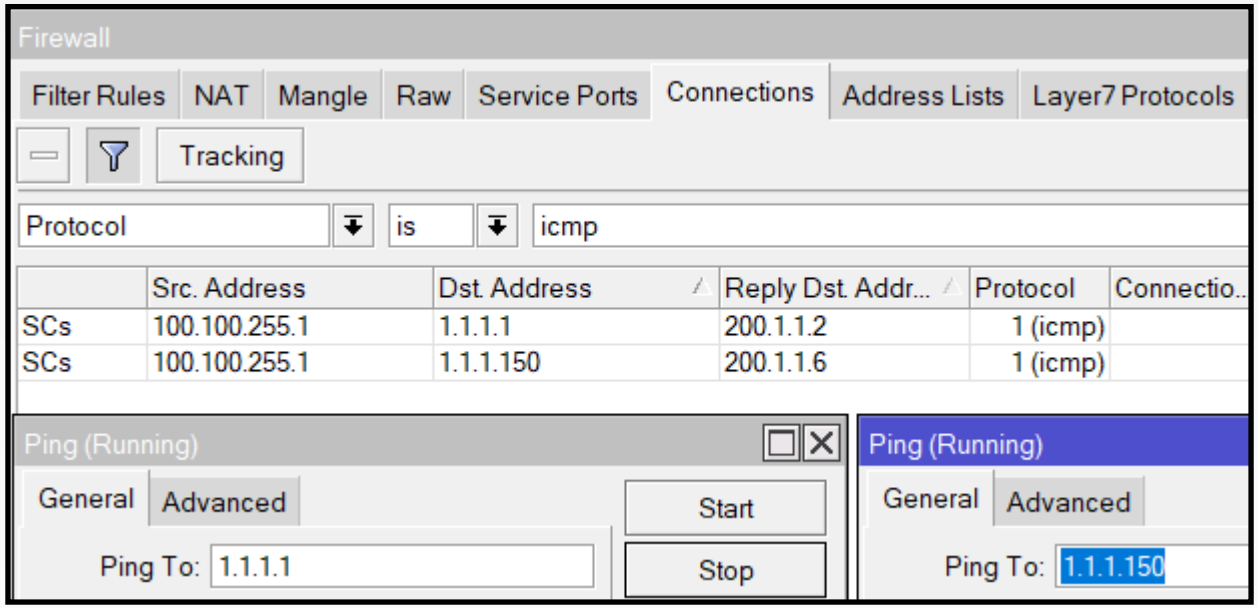
- Para não ter problemas com algumas aplicações, lembre-se de marcar a opção not-by-dst pois dessa forma o NAT irá olhar somente para o IP de origem do pacote para escolher o IP de tradução (resumindo um cliente sempre ficará preso a um único IP público).

Problemas com SAME

Redes Brasil

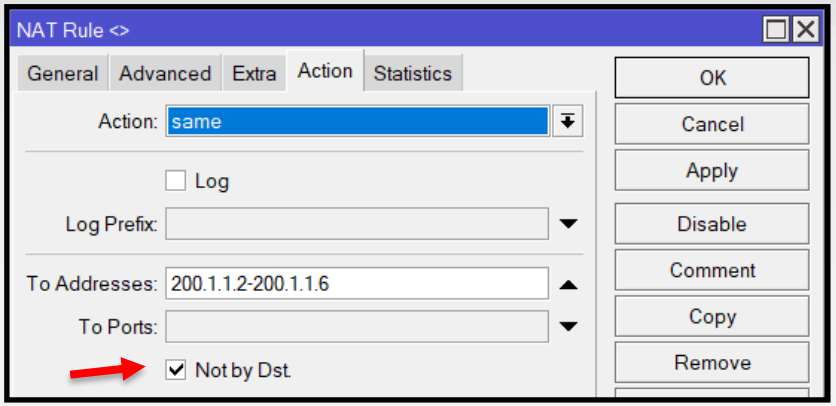
- As conexões com mesmo IP origem e com mesmo IP de destino sempre usarão o mesmo IP público;
- Se o IP de destino for diferente, um novo IP público poderá ser escolhido e isto poderá causar problemas em algumas aplicações.

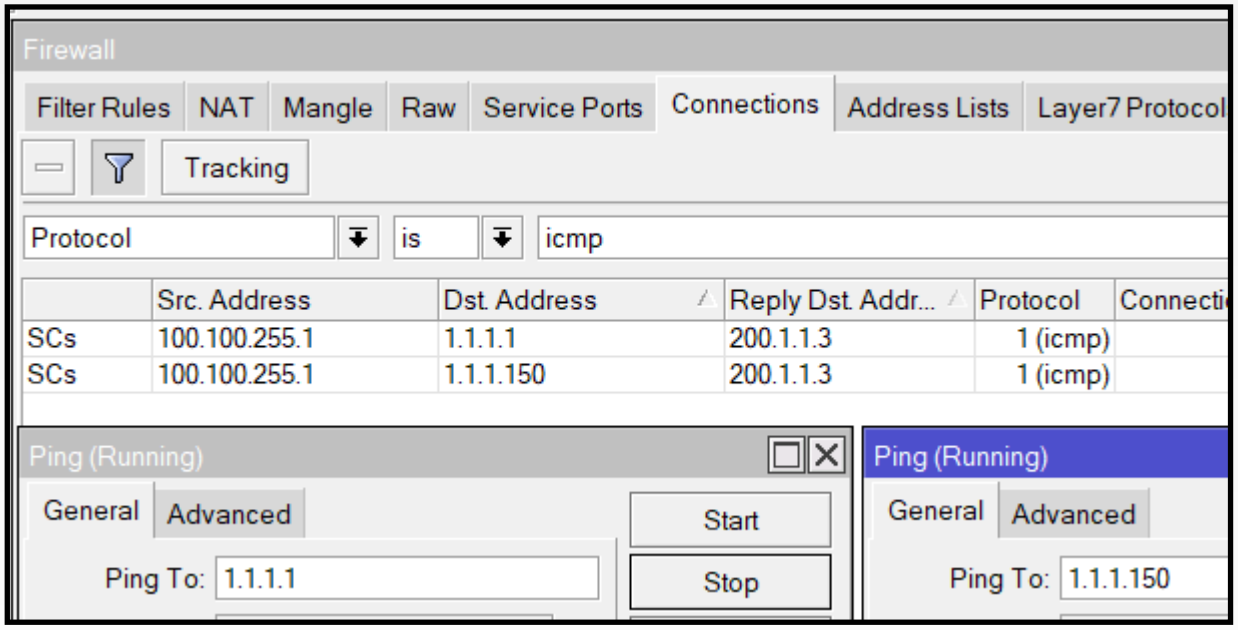




CGNAT com SAME

- Independente do destino as conexões de um mesmo cliente sempre usara o mesmo IP público para fazer as traduções.





CGNAT com ação NETMAP

- Indicado quando irá usar uma sub-rede inteira de IPs públicos na mesma regra, para as traduções dos IPs privados.

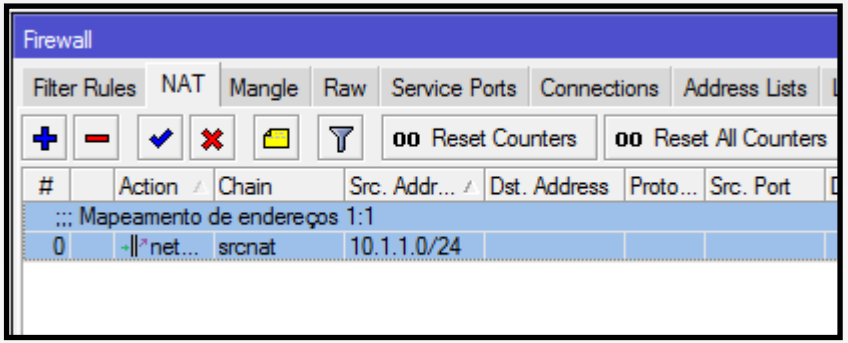
- O NET-MAP faz literalmente um mapeamento de IPs (1:1 ou 1:N) e dessa forma permite a fácil localização de IPs privados que fizeram uso de um IP público.

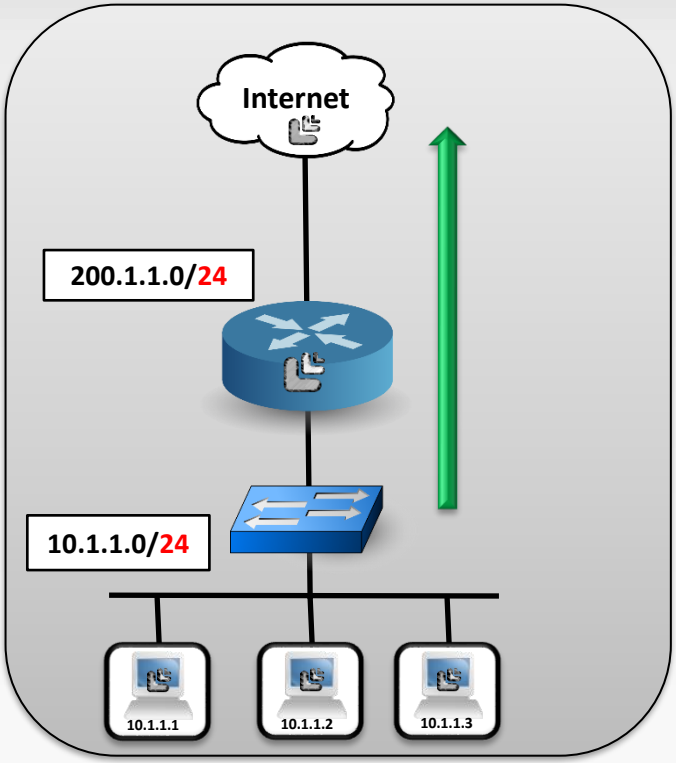
Usando a ação NET-MAP

Redes Brasil

- **NETMAP com sub-redes iguais**

10.1.1.0/24 mapeada na rede 200.1.1.0/24





Comandos

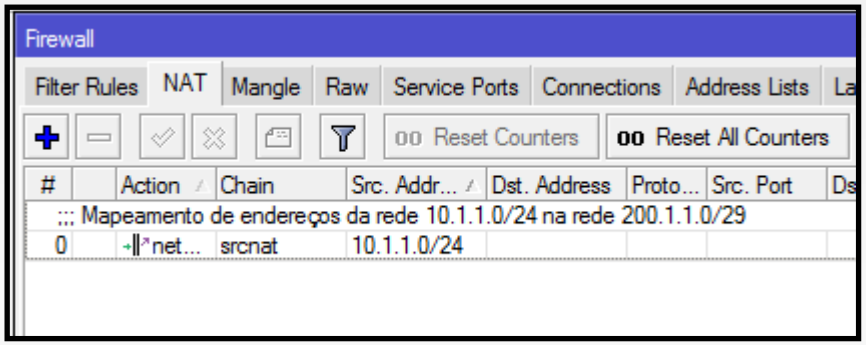
```
/ip firewall nat
add action=netmap chain=srcnat comment="Mapeamento de endere\E7os 1:1" dst-address-list=!rede-local dst-address-type=!multicast src-address=10.1.1.0/24 to-addresses=\
    200.1.1.0/24
```

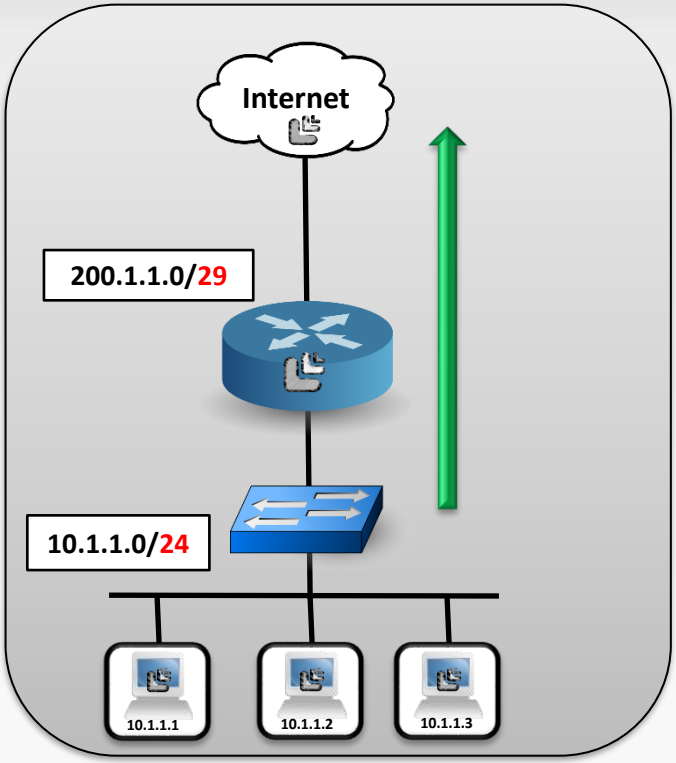
Usando a ação NET-MAP

Redes Brasil

- **NETMAP com sub-redes iguais**

10.1.1.0/24 mapeada na rede 200.1.1.0/29





Comandos

```
/ip firewall nat
add action=netmap chain=srcnat comment="Mapeamento de endere\E7os da rede 10.1.1.0/24 na rede 200.1.1.0/29" dst-address-list=!rede-local dst-address-type=!multicast \
   src-address=10.1.1.0/24 to-addresses=200.1.1.0/29
```

Mapeamento do NETMAP

Redes Brasil

Rede privada: **10.1.1.0/24**

Mapeada em uma

Rede pública: **200.1.1.0/29**

IP PRIVADO	IP PUBLICO
10.1.1.0	200.1.1.0
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2
10.1.1.3	200.1.1.3
10.1.1.4	200.1.1.4
10.1.1.5	200.1.1.5
10.1.1.6	200.1.1.6
10.1.1.7	200.1.1.7
10.1.1.8	200.1.1.0
10.1.1.9	200.1.1.1
10.1.1.10	200.1.1.2
10.1.1.11	200.1.1.3
10.1.1.12	200.1.1.4
10.1.1.13	200.1.1.5
10.1.1.14	200.1.1.6
10.1.1.15	200.1.1.7
10.1.1.16	200.1.1.0
10.1.1.17	200.1.1.1
10.1.1.18	200.1.1.2
10.1.1.19	200.1.1.3
10.1.1.20	200.1.1.4
10.1.1.21	200.1.1.5
10.1.1.22	200.1.1.6
10.1.1.23	200.1.1.7

200.1.1.0/29

200.1.1.0/29

200.1.1.0/29

Me ajuda ai vai!!

Me ajuda ai vai!!

SRC-NAT

- Pode ser usado para um CGNAT rápido com alocação de portas dinâmicas (lembrando de ter somente 1 IP no campo to-address em cada regra);
- Pode ser usado para fazer alocação de portas de estáticas para cada IP privado (2 regras para cada IP privado);

SAME

- Ideal para CGNAT rápido com alocação de portas dinâmicas e poderá ter um pool ou sub-rede de IPs no campo to-address.
- Lembre-se de marcar o not-by-dst para evitar problemas

NET-MAP

- Ideal para CGNAT com alocação estática de portas;
- Número de regras bem reduzido em relação ao SRC-NAT;

Cronograma Aulão NAT e CGNAT

Redes Brasil

- Porque usar NAT e porque CGNAT?
- Os canais do NAT do MikroTik RouterOS.
- Entendendo como funciona o SRC-NAT + boas práticas.
- Entendendo como funciona o DST-NAT + boas práticas.
- Topologias para CGNAT.
- Exemplos práticos de CGNAT com e sem uso de logs.
- Bônus final

Exemplo de localização do cliente

Redes Brasil

Gerador de CGNAT

Redes Brasil

100.92.210.0/23

200.1.1.0/28

Criar Regras

Informações

512 IPs privados.

16 IPs públicos.

32 clientes por IP público.

2016 portas por cliente.

Downloads

Regras para MikroTik

Relatório para acompanhamento

Exemplo de localização do cliente

1. É necessário a porta de origem ,IP público, data e hora da conexão.
2. Faça um filtro no relatório usando o IP público solicitado.
3. Faça um filtro no relatório para o range de portas levando em consideração a porta de origem solicitada.
- Agora você encontrou o IP privado que originou a conexão.
- Por ultimo consulte no seu sistema de gerenciamento qual foi o cliente que fez uso desse IP privado na data e hora solicitada.

Exemplo de localização do cliente

Redes Brasil

Identifique o cliente da seguinte conexão:

IP Público: **200.1.1.8**
Porta de origem: **58123**
Data: **15/01/2020**
Hora: **13:20:04**

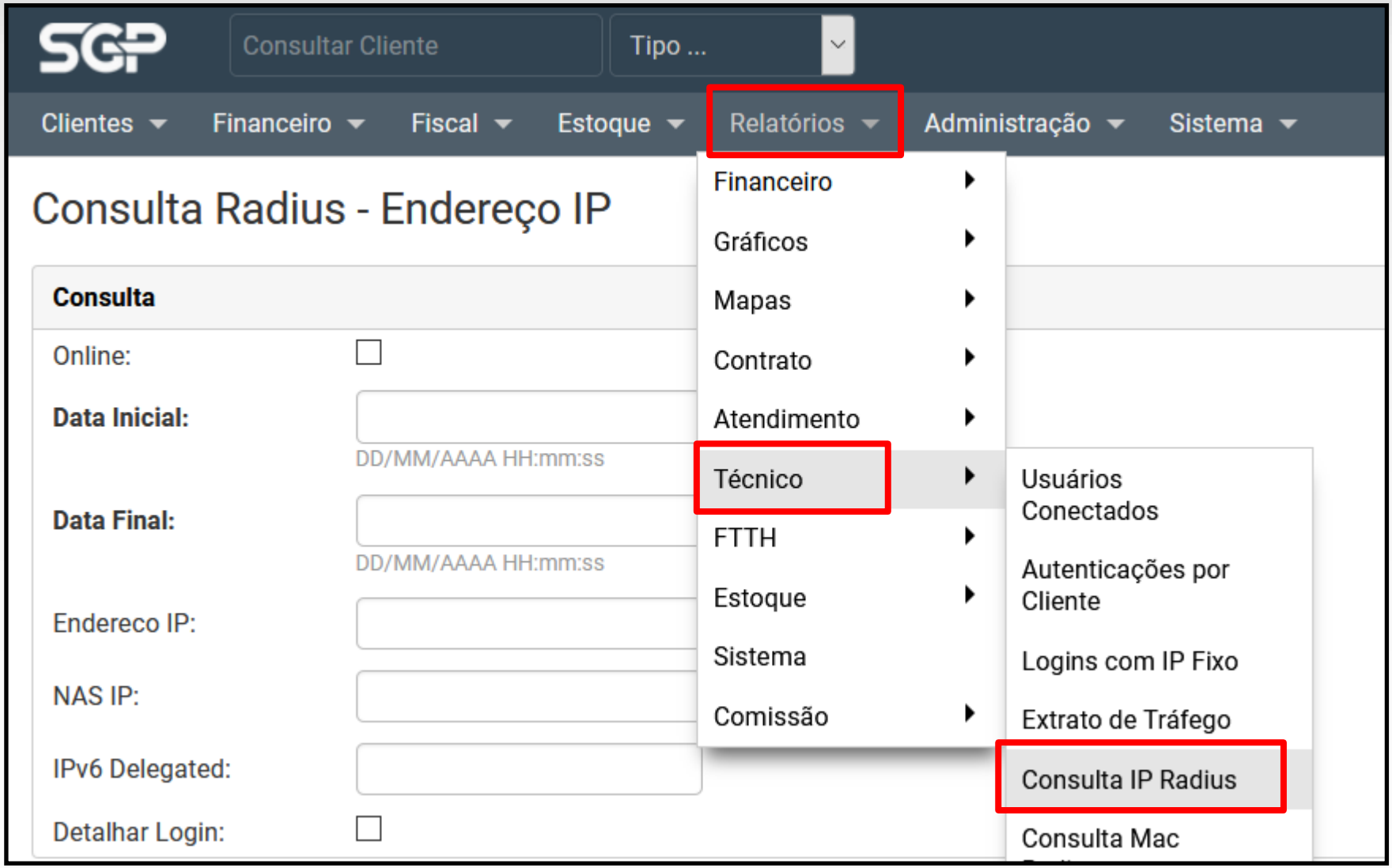
Portas	Bloco_Publico	Bloco_Privado
1024-3039	200.1.1.0	100.92.210.0
1024-3039	200.1.1.1	100.92.210.1
1024-3039	200.1.1.2	100.92.210.2
1024-3039	200.1.1.3	100.92.210.3
1024-3039	200.1.1.4	100.92.210.4
1024-3039	200.1.1.5	100.92.210.5
1024-3039	200.1.1.6	100.92.210.6
1024-3039	200.1.1.7	100.92.210.7
1024-3039	200.1.1.8	100.92.210.8
1024-3039	200.1.1.9	100.92.210.9
1024-3039	200.1.1.10	100.92.210.10
1024-3039	200.1.1.11	100.92.210.11
1024-3039	200.1.1.12	100.92.210.12
1024-3039	200.1.1.13	100.92.210.13
1024-3039	200.1.1.14	100.92.210.14
1024-3039	200.1.1.15	100.92.210.15
3040-5055	200.1.1.0	100.92.210.16
3040-5055	200.1.1.1	100.92.210.17
3040-5055	200.1.1.2	100.92.210.18
3040-5055	200.1.1.3	100.92.210.19
3040-5055	200.1.1.4	100.92.210.20
3040-5055	200.1.1.5	100.92.210.21
3040-5055	200.1.1.6	100.92.210.22
3040-5055	200.1.1.7	100.92.210.23
3040-5055	200.1.1.8	100.92.210.24

Portas	Bloco_Publico	Bloco_Privado
1024-3039	200.1.1.8	100.92.210.8
3040-5055	200.1.1.8	100.92.210.24
5056-7071	200.1.1.8	100.92.210.40
7072-9087	200.1.1.8	100.92.210.56
9088-11103	200.1.1.8	100.92.210.72
11104-13119	200.1.1.8	100.92.210.88
13120-15135	200.1.1.8	100.92.210.104
15136-17151	200.1.1.8	100.92.210.120
17152-19167	200.1.1.8	100.92.210.136
19168-21183	200.1.1.8	100.92.210.152
21184-23199	200.1.1.8	100.92.210.168
23200-25215	200.1.1.8	100.92.210.184
25216-27231	200.1.1.8	100.92.210.200
27232-29247	200.1.1.8	100.92.210.216

Portas	Bloco_Publico	Bloco_Privado
57472-59487	200.1.1.8	100.92.211.200

Exemplo para achar usuário no SGP

Redes Brasil



Exemplo para achar usuário no SGP

Redes Brasil

Identifique o cliente da seguinte conexão:

~~IP Público: **200.1.1.8**~~

~~Porta de origem: **58123**~~

Data: **15/01/2020**

Hora: **13:20:04**

IP privado encontrado no relatório:**100.92.211.200**

Cronograma Aulão NAT e CGNAT

Redes Brasil

- Porque usar NAT e porque CGNAT?
- Os canais do NAT do MikroTik RouterOS.
- Entendendo como funciona o SRC-NAT + boas práticas.
- Entendendo como funciona o DST-NAT + boas práticas.
- Topologias para CGNAT.
- Exemplos práticos de CGNAT com e sem uso de logs.
- Bônus final

Dúvidas e perguntas